REMARKS

Claim Amendments

Applicants respectfully request entry of the foregoing claim amendments, which amend independent Claims 1 and 20 to include the features of dependent Claims 3 and 22. Dependent Claims 3 and 22 are now canceled, and dependent Claims 4, 23, and 35 are amended accordingly. No new matter is introduced.

Rejections under 35 U.S.C. § 103

Claims 1-2, 7-8, 16-19, 20-21, 25-26, and 34-37 are rejected under 35 U.S.C. § 103 due to U.S. Pat. No. 6,081,793 of Challener *et al.* (here, "Challener *et al.*") in view of U.S. Pat. No. 5,903,652 of Mital (here, "Mital"), and further in view of the article "How to Share a Secret" by Adi Shamir, from the *Communications of the ACM*, November 1979, Vol. 22, No. 11 (here, "Shamir").

Remaining dependent claims 4, 9-12, 23, and 27-30 are rejected over Challener *et al.* in view of Mital and Shamir as applied to independent Claims 1 and 20, and further in view of Schneier (cited in previous Office Action); dependent claims 13-15, 31-33, and 38 are rejected over Challener *et al.* in view of Mital and Shamir, and further in view of Ansell *et al.* (cited in previous Office Action); and dependent claim 39 is rejected over Challener *et al.* in view of Mital and Shamir, and further in view of Coss *et al.* (EP 0 909 074 A1).

As discussed below, Applicants respectfully traverse these rejections and request reconsideration and allowance of all claims.

Independent Claims 1 and 20

Applicants respectfully submit that neither Challener *et al.* nor Mital discloses or suggests the communication module and mapping module as claimed in independent Claims 1 and 20, as amended.

Figs. 9A-9D of Challener *et al.* are block diagrams of the encryption operations performed by a computer-moderated voting system, which occur in several successive steps, as described at Col. 9, line 28 through Col. 11, line 3. First, in Fig. 9B, a voter computer sends a

request for a ballot, along with a voter ID, to an authentication server. Next, in Fig. 9C, the authentication server returns a ballot to the voter. Next, in Fig. 9D, several steps occur. First, the voter submits a completed vote and voter ID to the authentication server. The authentication server backs up a copy of the voter's submission to a journal server; and, having confirmed the voter's qualifications, forwards the completed vote to a ballot counter with an "add" message. The authentication server also returns a copy of the completed vote to the voter.

None of these steps, taken individually or together, disclose or suggest the claimed communication module and mapping module of independent Claims 1 and 20, as amended.

First, Fig. 9B does not disclose or suggest the claimed communication module and mapping module. In Fig. 9B, the voter sends a request for ballot, encrypted with the voter's private key VO, and the voter's ID, encrypted with the authentication server's public key AX, to the authentication server. In this transmission, the voter's computer does not act as the claimed communication module and mapping module, because the voter's computer is not transmitting both an anonymously mapped identifier portion and an unmapped research data portion of working data to the authentication server, as required by the independent claims ("wherein the communication module is capable of transmitting both the anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver"). Instead, there is no "anonymously mapped" portion of this voter transmission, because the authentication server is intended to read the voter ID in order to verify that the voter is eligible and properly identified (see Col. 9, lines 51-55), and also to read the request for ballot in conjunction with the voter's private key in order to verify that the request is from the voter and not an imposter (see Col. 9, lines 60-62).

Next, Fig. 9C likewise does not disclose or suggest the claimed communication module or mapping module, because it shows only the transmission of a ballot from the authentication server back to the voter. Fig. 9C therefore does not disclose or suggest transmitting both an anonymously-mapped identifier portion and an unmapped research data portion of working data to the authentication server, as required by the independent claims.

Next, none of the transmissions in Fig. 9D, separately or together, discloses or suggests the claimed communication module.

First, the voter transmits a completed vote and voter ID to the authentication server. In this transmission, the voter's computer does not act as the claimed communication module or mapping module because it does not transmit an anonymously-mapped identifier, as required by the independent claims. The voter ID is not anonymously-mapped, because it is used by the authentication server to verify that the vote is from the voter (see Col. 10, lines 14-15); and the completed vote is not an anonymously-mapped identifier, because it is packaged in the voter's private key VO so that the authentication server can verify that it is from the voter (see Col. 10, lines 14-15).

Next, the authentication server transmits a copy of the completed vote and voter ID to the journal server (see Col. 10, lines 20-21). In doing so, the authentication server likewise does not act as the claimed communication module or mapping module because the transmission is the same as the one previously discussed (from the voter to the authentication server), and therefore lacks an anonymous mapping for the same reasons.

Next, the authentication server sends the completed vote and an "add" message to the ballot counter (see Col. 10, lines 22-27). In doing so, the authentication server likewise does not act as the claimed communication module or mapping module because the completed vote and "add" message are accessed by the ballot counter, and therefore neither part of the transmission could be considered "anonymously-mapped."

Finally, the authentication server sends a copy of the completed vote to the voter (see Col. 10, lines 27-31). In doing so, the authentication server likewise cannot be acting as the communication module or mapping module because only the completed vote is transmitted, and not both an anonymously-mapped identifier portion and an unmapped research data portion of working data, as required by the claims of the present invention.

Further, the authentication server does not act as the claimed communication and mapping modules, by taking the transactions of Fig. 9D as a whole. That is, consider that the authentication server receives the completed vote and voter ID; and later forwards the completed vote and "add" message to the ballot counter. In doing so, the authentication server cannot access the completed vote, because the completed vote is encrypted with the ballot counter's private key. It therefore cannot be acting as the claimed mapping module, because it is not "capable of accessing both the identifier portion and the research data portion of the working

data," as required by the independent claims. Further, the authentication server cannot be acting as the claimed communication module because the completed vote and "add" message are accessed by the ballot counter, and therefore neither part of the transmission could be considered "anonymously-mapped" as required by the independent claims ("wherein the communication module is capable of transmitting both the anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver").

Figs. 9A-9D of Challener *et al.* therefore do not disclose or suggest the claimed communication module and mapping module of independent Claims 1 and 20.

Likewise, Mital does not disclose or suggest the claimed communication module and mapping module. As shown in Figs. 1, 13A and 13B, Mital involves a consumer computer 100 sending a secure purchase order message 102 to an electronic commerce service 104. The secure purchase order message 102 includes an auditing attachment, a goods and services order, and payment instructions. The electronic commerce service 104 removes the auditing attachment, and forwards the goods and services order and payment instructions to a merchant computer 108. The merchant computer 108 accesses the goods and services order, and forwards the payment instructions to an acquirer computer 112 in order to obtain payment authorization. Once payment authorization is received, the merchant computer 108 generates a receipt message 116 that is forwarded to the consumer computer 100.

The Office Action states, at Page 4, last paragraph, that Mital discloses a communication module that is capable of transmitting both an anonymously mapped identifier portion and an unmapped research data portion of working data to a receiver, referring to Col. 7, line 65 through Col. 8, line 14. This passage describes the consumer computer 100 encrypting the audit information, goods and service order, and payment instructions into different encryption formats to ensure that only the online network provider, merchant, and credit provider can access their respective portions of the purchase order message 102. However, in forming the purchase order message 102, the consumer computer 100 does not act as the claimed communication module because it does not create the "secure communication channel" recited in independent Claims 1 and 20, as amended: "a communication module... for establishing a communication connection... wherein the communication connection is a secure communication channel formed by the communication module (i) authenticating the sender and receiver, resulting in an

authorized sender and authorized receiver, and (ii) encrypting working data transmitted over the channel." In particular, the consumer computer 100 does not establish a secure communication connection between a sender and a receiver, over which encrypted working data is transmitted, by authenticating both the sender and the receiver, as required by amended independent Claims 1 and 20. Instead, the consumer computer 100 transmits its purchase order message 102 over publicly accessible network 106. Thus, Mital does not disclose or suggest the claimed communication module.

Next, the Office Action states at Page 4, last line through Page 5, second line, that Mital discloses a mapping module that is capable of accessing both the identifier portion and the research data portion of the working data at Col. 27, lines 54-61 of Mital. At that passage, Mital describes the consumer computer 100 encrypting the payment instructions portion of the purchase order message 102. The Office Action therefore appears to take the consumer computer 100 as including a mapping module that is anonymously mapping the payment instructions that are transmitted to the electronic commerce service 104, which would therefore be taken as the receiver. However, if the electronic commerce service 104 is taken as the receiver, the consumer computer 100 would also need to include a communication module for establishing a secure communication connection between a sender and the electronic commerce service 104, as required by the amended independent claims. Since, as described above, the consumer computer 100 does not act to create the claimed secure communication connection, it therefore cannot be taken to include the communication module; and the assumption that the consumer computer 100 could act as the mapping module therefore could not consistently satisfy both the communication module and mapping module terms of the independent claims.

Applicants therefore respectfully submit that neither Challener *et al.* nor Mital discloses or suggests the communication module and mapping module required by independent Claims 1 and 20, as amended.

Likewise, Shamir also does not disclose or suggest the communication module and mapping module, since it is directed entirely to an algorithm for secret sharing. Thus, since Shamir does not remedy the lack of disclosure or suggestion of the other two references, Applicants respectfully submit that none of the references discloses or suggests the features of independent Claims 1 and 20. In addition, because it does not disclose or suggest Applicants'

claimed mapping module and communication module, Shamir necessarily does not disclose or suggest the use of secret sharing to control access to Applicants' claimed mapping module.

Therefore, because Challener *et al.* in view of Mital, and further in view of Shamir does not disclose or suggest the inventions of independent Claims 1 and 20, Applicants respectfully request reconsideration and allowance of those claims.

Dependent Claims

In addition, because dependent claims 2, 7-8, 16-19, 21, 25-26, and 34-37 incorporate the features of base claims 1 and 20, they are also allowable for the foregoing reasons.

Also, neither Schneier, nor Ansell *et al.*, nor Coss *et al.*, which are applied to several of the dependent claims, discloses or suggests the foregoing features. In particular, those references do not disclose or suggest a communication module and mapping module as claimed in the independent claims, nor the use of secret sharing to control access to Applicants' claimed mapping module; nor the preceding three features in combination.

Applicants therefore submit that remaining dependent claims 4, 9-15, 23, 27-33, 38, and 39 are also allowable for the foregoing reasons.

Claims 40 and 41

Claims 40 and 41 were not addressed in the Office Action, although they were listed as rejected in the check-boxes on page 1 of the Office Action. Therefore, for the sake of clarity, Applicants submit that Claims 40 and 41 are also allowable for the reasons given above for their respective base claims 1 and 20, and request reconsideration and allowance of those claims.

Construction of the Term "Working Data Identifier Set Domain"

Applicants respectfully traverse the statements in the Office Action at Page 2, last paragraph, and Page 4, first full paragraph, regarding the definition of "working data identifier set domain."

Applicants have submitted that the claim term "working data identifier set domain" should be interpreted to require a domain, which is associated with an identifier set, which is associated with working data.

In response, the Office Action maintains that such a construction is not permissible because the claim language does not claim "a domain which is associated with an identifier set and which is associated with working data."

Applicants respectfully submit that it is not required for claim terms to use exactly the same words as their construction. Claims often use words or phrases whose constructions are longer sentences than the words in the claims themselves. The inter-relationship of claim terms, for example, necessarily implies more meaning than the terms separately.

Thus, by placing the portions of the claim term "working data identifier set domain" together in a single phrase, it is implied that the portions of the claim term should be construed as being "associated with" each other.

In addition, although it is true that during examination, claims must be interpreted as broadly as their terms reasonably allow, that does not mean that words in the claim may be ignored. The construction of "working data identifier set domain" found at Page 4, first full paragraph of the Office Action ("data that devices process that are divided into sets") impermissibly ignores several words in the claim term, such as "identifier" and "domain," and essentially truncates the words to be only "working data sets."

Thus, Applicants respectfully submit that the claim term "working data identifier set domain" should not be construed as given at Page 4, first full paragraph of the Office Action, but rather, based on the words of the claim themselves, should involve 1) a domain; which is 2) associated with an identifier set; which is 3) associated with working data. Such a construction is consistent with the prosecution history made of record (see RCE-Amendment filed June 30, 2005, Remarks section, Page 9).

Using such a construction, Applicants submit that the claims are not disclosed or suggested by the cited art for the reasons given above, which are, in any event, valid reasons independent of the exact construction of this claim term.

CONCLUSION

In view of the above remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By _____
Keith J. Wood
Registration No. 45,235
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 10/26/06